Comment Form

Date	Document
11/15/02	Guidance for Industry 21 CFR Part 11; Electronic Records; Electronic Signatures Maintenance

Commenter	Section	Paragraph Figure/ Table Line No.	Proposed Change	Comment/ Rationale
		Line #121-125	Change from: ...into several broad categories. Examples of such categories include but are not limited to... To: ...into several broad categories. Predicate Rule requirements vary. Depending upon the regulated industry, Predicate Rules may include, but are not limited to...	To clarify the requirements for an Archive, the GLPs require not only retention of study records, but also: "There shall be archives for orderly storage and expedient retrieval of all raw data, documentation, protocols, specimens, and interim and final reports. Conditions of storage shall minimize deterioration of the documents or specimens in accordance with the requirements for the time period of their retention and the nature of the documents or specimens. A testing facility may contract with commercial archives to provide a repository for all material to be retained. Raw data and specimens may be retained elsewhere provided that the archives have specific reference to those other locations." "An individual shall be identified as responsible for the archives" "Only authorized personnel shall enter the archives" "Material retained or referred to in the archives shall be indexed to permit expedient retrieval" Clearly these requirements were written with paper in mind, but this is still the predicate rule so we cannot maintain electronic records on the computer or system on which they were generated. They must be 'archived' off to another system or media. This requirement seems to conflict with lines 243-245 which more or less suggests/recommends a separate archive to be 'prudent'. This guidance should not be interpreted in a manner which would expand the scope of Predicate Rules across FDA divisions.
		Line #152-182	Delete	This is redundant, as these requirements are already stated in the regulation.

				Date 11/15/02	Document Guidance for Industry 21 CFR Part 11; Electronic Records; Electronic Signatures Maintenance
Commenter	**Section**	**Paragraph Figure/ Table Line No.**	**Proposed Change**	**Comment/ Rationale**	
		Line #210-211	From: You should identify and control factors that could potentially affect the reliability of electronic records during their records retention period. To: Factors that could potentially affect the reliability of electronic records during their record retention periods should be identified in the User Requirements Specification and Risk Assessment Process.	This has no meaning independent from what companies already do as a part of system validation. This is managed through the Risk Assessment process and User Requirements Definition.	
		Lines #227-235	Change Lines 227-229 (the first sentence in this section) From: As Is To: Continued availability of electronic record information should be addressed through periodic testing. Also, delete lines 229-235. For example, if...in this regard.	This is done on a process basis not a record basis. That is, tests are performed to determine if we can read records on a tape. We don't see if we can read specific records. This is a very important distinction from a process point of view. In this same section is a reference to suppliers and producers of media. If you analyze history, the likelihood of the supplier outliving the e-record is unlikely. This also implies that suppliers may incur legal liability. To establish a system to periodically retrieve information (based on a time period) will require vast resources. What is meant by a representative number of electronic records? Is it a valuable utilization of resources to keep all the electronic files 'viable'? This is an area where a risk based approach would help considerably. To put a process into place based upon guidance will require significant resources, but not reduce risk by a significant amount.	
		Line #236-245	Delete	This may be a good business practice; however, very little specific, concrete guidance is provided. Also, the terminology "most important electronic records" and "primary electronic records" is unclear and actually creates questions rather than providing guidance.	

Date	Document
11/15/02	Guidance for Industry 21 CFR Part 11; Electronic Records; Electronic Signatures Maintenance

Commenter	Section	Paragraph Figure/ Table Line No.	Proposed Change	Comment/ Rationale
		Line #250	From: "You should monitor the conditions under which..." To: "You should consider the conditions under which..."	The requirement in the guidance document to monitor the conditions under which the electronic records are stored (giving recommended parameters to measure such as temperature, humidity, dust, vibration, and sources of electromagnetic and radio frequency interference) adds unnecessary requirements for record storage and retrievability. Retrievability of the electronic records during their retention period should be verified; the monitoring of environmental records should be voluntary as needed.
		Line #291	From: "...incomplete copy from Draft Guidance For Industry --Not For Implementation 12 being..." To: "incomplete copy from being..."	Contains extraneous words that look as though they were once the footer for the document. Eliminate 'Draft.....12.'
		Line #334-336	Delete: "You should document the migration so that you have a traceable history of what systems were used throughout the records retention period."	A systems history is maintained via change control for validated systems. But, once records are migrated to a "new" system, the information about the old system is immaterial. This would include operating systems and other infrastructure components.
		Line #337-354	Delete: "Upon completion and verification...preserve and present information."	Delete this section. "Old" e-records are deleted or purged when the record migration to a "new" system has been completed. Record migration is validated. The ability to process "old" e-records is not a viable option. This is the purpose for validating the migration process.
		Line #427-429	Delete: "An audit trail itself may undergo...and/or deletion of an old electronic record."	Delete. Adds no new guidance.
		Line #471-487	Delete this entire section: "Just prior to performing...migrated electronic record and explanatory statement."	This entire section is confusing. Migration is a validated process. There is no clarity as to what constitutes a "trusted third party." This concept adds additional process steps without a corresponding increase in data integrity from a risk management perspective.
		Line #488-499	Delete this section: "Color code changes; the electronic record...the record content and authenticity."	This is a specific feature which is typically not supported in software applications. It appears to state unnecessary, additional process steps without a corresponding increase in the integrity of records which are migrated (from a risk management perspective.)

Guidance for Industry

21 CFR Part 11; Electronic Records; Electronic Signatures

Maintenance of Electronic Records

Draft Guidance

This guidance document is being distributed for comment purposes only.

Comments and suggestions regarding this draft document should be submitted within 90 days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance. Submit comments to Dockets Management Branch (HFA-305), Food and Drug Administration, 5630 Fishers Lane, room 1061, Rockville, MD 20852. All comments should be identified with the docket number 00D-1539.

For questions regarding this draft document contact Paul J. Motise, Office of Enforcement, Office of Regulatory Affairs, 301-827-0383, e-mail: pmotise@ora.fda.gov.

U.S. Department of Health and Human Services
Food and Drug Administration
Office of Regulatory Affairs (ORA)
Center for Biologics Evaluation and Research (CBER)
Center for Drug Evaluation and Research (CDER)
Center for Devices and Radiological Health (CDRH)
Center for Food Safety and Applied Nutrition (CFSAN)
Center for Veterinary Medicine (CVM)
July 2002

Guidance for Industry

21 CFR Part 11; Electronic Records; Electronic Signatures

Maintenance of Electronic Records

Additional copies of this draft guidance document are available from the Office of Enforcement, HFC-200, 5600 Fishers Lane, Rockville, MD 20857; Internet http://www.fda.gov/ora/compliance_ref/part11/default.htm

U.S. Department of Health and Human Services
Food and Drug Administration
Office of Regulatory Affairs (ORA)
Center for Biologics Evaluation and Research (CBER)
Center for Drug Evaluation and Research (CDER)
Center for Devices and Radiological Health (CDRH)
Center for Food Safety and Applied Nutrition (CFSAN)
Center for Veterinary Medicine (CVM)
July 2002

Guidance For Industry

21 CFR Part 11; Electronic Records;

Electronic Signatures

Maintenance of Electronic Records

Table of Contents

Guidance For Industry[1]

21 CFR Part 11; Electronic Records; Electronic Signatures

Maintenance of Electronic Records

This draft guidance, when finalized, will represent the Food and Drug Administration's (FDA's) current thinking on this topic. It does not create or confer any rights for or on any person and does not operate to bind FDA or the public. An alternative approach may be used if such approach satisfies the requirements of applicable statutes and regulations.

1. Purpose

The purpose of this draft guidance is to describe the Food and Drug Administration's (FDA's) current thinking regarding principles and procedures for maintaining electronic records in electronic form in meeting the requirements of Part 11 of Title 21 of the Code of Federal Regulations; Electronic Records; Electronic Signatures. It provides guidance to industry, and is intended to assist persons who are subject to the rule to comply with the regulation. It may also assist FDA staff who apply part 11 to persons who are subject to the regulation.

[1] This draft guidance was prepared under the aegis of the Office of Enforcement by the FDA Part 11 Compliance Committee. The committee is composed of representatives from each center within the Food and Drug Administration, the Office of Chief Counsel and the Office or Regulatory Affairs.

95 2. Scope

96 This draft guidance is one of a series of guidances about part 11. We intend to provide
97 information with respect to FDA's current thinking on acceptable ways of meeting part 11
98 requirements to ensure that electronic records and electronic signatures are trustworthy,
99 reliable, and compatible with FDA's public health responsibilities. This draft guidance
100 focuses on maintenance of electronic records.

101 When an FDA regulation requires that a record be maintained, generally the regulation
102 specifies the period of time the record must be kept (referred to in this draft guidance as
103 the records retention period). We intend this draft guidance to apply to the entire required
104 retention period regardless of how actively the records are used or accessed.

105 This draft guidance presents key principles and practices and addresses some frequently
106 asked questions, but it is not intended to cover everything about maintaining electronic
107 records. The guidance provides two examples of approaches to electronic record
108 maintenance.

109 This document includes some considerations that are also relevant to recording
110 information in the first place. If information is inaccurately or incompletely
111 recorded, record maintenance practices will not compensate for those shortcomings.

112 ***2.1 Applicability***

113 Part 11 applies to electronic records and electronic signatures that persons create, modify,

115 maintain, archive, retrieve, or transmit under any records or signature requirement set
116 forth in the Federal Food, Drug, and Cosmetic Act (the Act), the Public Health Service
117 Act (PHS Act), or any FDA regulation. Any requirements set forth in the Act, the PHS
118 Act, or any FDA regulation, with the exception of part 11, are referred to in this
119 document as predicate rules. Most predicate rules are contained in Title 21 of the Code of
120 Federal Regulations. In general, predicate rules address the research, production, and
121 control of FDA regulated articles, and fall into several broad categories. Examples of
122 such categories include, but are not limited to: manufacturing practices, laboratory
123 practices, clinical and pre-clinical research, adverse event reporting, product
124 tracking, and pre and post marketing submissions and reports. However, this draft
125 guidance only applies to records that, by predicate rule, you are required to maintain.

126 ***2.2 Audience***

127 We intend this draft guidance to provide useful information and recommendations to:

128 • Persons subject to part 11;
129 • Persons responsible for the maintenance of electronic records; and,
130 • Persons who develop products or services to enable implementation of part 11
131 requirements;

132 This draft guidance may also assist FDA staff who apply part 11 to persons subject to the
133 regulation.

134 3. Definitions and Terminology

135 Unless otherwise specified below, all terms used in this draft guidance are defined in

137 FDA's draft guidance document, "Guidance For Industry, 21 CFR Part 11; Electronic
138 Records; Electronic Signatures, Glossary of Terms," a document common to the series of
139 guidances on part 11.

140 ## 4. Regulatory Requirements

141 ### *4.1 What Does Part 11 Require?*

142 Part 11 has several requirements relevant to maintenance of electronic records. For
143 example:

144 • Section 11.10 requires persons to "employ procedures and controls designed to
145 ensure the authenticity, integrity, and, when appropriate, the confidentiality of
146 electronic records, and to ensure that the signer cannot readily repudiate the
147 signed record as not genuine." To satisfy this requirement persons must, among
148 other things, employ procedures and controls that include "[P]rotection of
149 records to enable their accurate and ready retrieval throughout the records
150 retention period." See section 11.10(c).

151 Other part 11 requirements apply throughout the record retention period. Therefore, you
152 should take the requirements below, among others, into account as you plan and
153 implement your electronic records maintenance activities. Here are some examples:

154 • Section 11.10(a): "Validation of systems to ensure accuracy, reliability,

156 consistent intended performance, and the ability to discern invalid or altered
157 records."

158 • Section 11.10(b): "The ability to generate accurate and complete copies of
159 records in both human readable and electronic form suitable for inspection,
160 review, and copying by the agency."

161 • Section 11.10(d): "Limiting system access to authorized individuals."
162
163 • Section 11.10(e): Use of secure, computer-generated, time-stamped, audit trails
164 that, among other things, "shall be retained for a period at least as long as that
165 required for the subject electronic records and shall be available for agency
166 review and copying."

167 • Section 11.50: Signed electronic records shall contain information associated
168 with the signing that clearly indicates the printed name of the signer, the date
169 and time of signing and what the signature means. These items shall be "subject
170 to the same controls as for electronic records and shall be included as part of
171 any human readable form of the electronic record (such as electronic display or
172 printout)." Accordingly, the signature manifestation information, associated
173 with an electronic record that is subject to this requirement, must be maintained
174 for the duration of the record retention period.

175 • Section 11.70: "Electronic signatures and handwritten signatures executed to
176 electronic records shall be linked to their respective electronic records to ensure

178 that the signatures cannot be excised, copied, or otherwise transferred to falsify
179 an electronic record by ordinary means."

180 Implementation of these and other part 11 controls will help to ensure that your
181 maintained electronic records will be trustworthy, reliable, authentic, and compatible
182 with FDA's public health responsibilities.

183 *4.2 What Do Predicate Rules Require?*

184 In addition to establishing records retention periods, predicate rules, among other
185 things, establish record content and signing requirements. It is beyond the scope of this
186 document to enumerate these requirements. However, keep in mind that electronic
187 records must still meet predicate rule content and signing requirements, and they must be
188 retained for as long as the predicate rule requires.

189 5. General Considerations For Electronic Records Maintenance

190 We believe it is very important that the factors unique to the maintenance of electronic
191 records are controlled and work properly together so that people can accurately and
192 readily retrieve and use the information that was originally intended to be preserved and
193 presented. We believe the following principles and practices will help meet that
194 objective.

5.1 Procedures For Electronic Records Maintenance Should Be Established and Followed.

As noted under Section 4 of this document, Section 11.10(c) requires that you employ procedures and controls for the protection of records to enable their accurate and ready retrieval throughout the records retention period. You should update the procedures and controls as conditions warrant. Procedures should describe:

- How electronic records will be maintained;
- Storage conditions and precautions;
- Retrieval and access restrictions;
- The technical approach to long term electronic record storage (e.g., electronic records migration, as described below); and,
- Personnel responsibilities for relevant tasks.

5.2.1 Factors That Might Affect The Reliability Of Electronic Records During the Required Retention Period Should Be Identified And Controlled.

You should identify and control factors that could potentially affect the reliability of electronic records during their records retention periods. These factors include, but are not limited to:

- Data encoded within an electronic record (e.g., computer readable representations of information);
- Metadata for an electronic record (e.g., information that gives the data meaning and context, such as data dictionaries for databases);
- Media (e.g., disk, tape, or flash memory devices) that record data and metadata;
- Hardware used to retrieve and display the electronic record;

220 • Software (both application programs and operating systems) used to read,
221 process, and display electronic records; and,
222 • The processes of extracting and presenting information in human readable form.
223 If these factors are not controlled properly the information that the electronic records
224 should convey might not be complete, accurate, or usable.

225 ***5.3 Continued Availability And Readability Of Electronic Record***
226 ***Information Should Be Ensured.***

227 You should periodically access a representative number of electronic records to ensure
228 that record contents can still be read and evaluated throughout the records retention
229 period. For example, if you store electronic records on reels of magnetic tape, you should,
230 on a pre-established schedule, rewind the tape and ensure you can still read the electronic
231 records. We believe that suppliers and producers of electronic recording media have
232 specific scientific information relating to the performance characteristics and limitations
233 of the media. Therefore, those suppliers and producers should be a good source of
234 information about how frequently you should try to access the electronic records.
235 Literature searches may also provide useful information in this regard.

236 If you find that you are starting to have difficulty reading the electronic records we
237 believe it would be highly advisable to subject them to data recovery procedures and/or
238 transcribe them onto fresh electronic recording media before the degradation renders the
239 electronic records unrecoverable. Because electronic records are generally more
240 perishable than traditional paper records, you should make back up electronic copies of

242 your most important electronic records and store them separately from the primary
243 electronic records. For example, we believe it would not be prudent to store both primary
244 and backup electronic records on the same computer hard drive because both could be
245 lost if the hard drive fails.

246 ***5.4 Electronic Records Should Be Stored Under Appropriate Environmental***
247 ***Conditions.***

248 You should determine what storage conditions are appropriate for the specific electronic
249 record media, and then maintain those conditions throughout the records retention period.
250 You should monitor the conditions under which the electronic records are stored. We
251 believe that suppliers and producers of recording media can be a good source of
252 information about specifications and precautions regarding such factors as temperature,
253 humidity, dust, vibration, and sources of electromagnetic and radio frequency
254 interference. Literature searches might also provide useful information about these
255 factors.

256 ***5.5 The Ability To Process An Electronic Record's Information Throughout Its***
257 ***Records Retention Period Should Be Preserved.***

258 Throughout the records retention period, the ability to process information in an
259 electronic record should not diminish. By being able to process the information, you
260 would maintain the ability, for example, to effectively and efficiently reconstruct events,
261 detect and investigate problems, detect trends and assess the need to modify procedures

263 or specifications to improve product quality, safety, and effectiveness. Some FDA
264 regulations require that records be maintained so that data in the records can be used for
265 periodically evaluating product quality standards to determine the need for changes in
266 product specifications, or manufacturing or control procedures – see 21 CFR 211.180(e),
267 for example. In addition, maintaining an electronic record in a form that permits the
268 record's information to be processed should help you to meet the part 11 requirement that
269 you be able to generate electronic copies of electronic records that are suitable for FDA
270 inspection, review, and copying. See section 11.10(b), as mentioned above in Section 4 of
271 this document. The ability to process information in an electronic record is a key aspect
272 of whether certain electronic records are suitable for FDA inspection and review.

273 Accordingly, where you could use computer technologies to search, sort, or manipulate
274 information in an original electronic record, you should be able to use computer
275 technologies to perform the same kinds of processing on information in the maintained
276 electronic record. For example, if you could automatically search for words in the text of
277 an electronic record, sort or find values in a table, or perform calculations in a
278 spreadsheet, you should be able to process information in a like manner for the electronic
279 record over the entire records retention period. This ability (or functionality) derives
280 largely from the hardware and software used to extract information from the electronic
281 record, as well as the electronic record format itself. You should include this ability
282 among your specifications in your procedures and controls.

284 *5.6 Copying Processes Should Produce Accurate And Complete Copies.*

285 You may find it necessary to copy electronic records from time to time during their
286 records retention periods (e.g., from one type of disk to the same or different
287 type of disk). One reason for this copying may be to compensate for wear and
288 tear on media. We believe that it is very important that information not be lost or
289 altered in the copy process. Some systems have a built-in copy verification mechanism,
290 such as a cyclic redundancy check, that could be used to prevent an inaccurate or
291 incomplete copy from Draft Guidance For Industry – Not For Implementation 12 being
292 made. A copy process that does not implement such a built-in error checking mechanism
293 to prevent making an inaccurate or incomplete copy should be validated.

294 6. Approaches To Maintenance Of Electronic Records

295 You should use an approach to maintenance of electronic records that is best suited to
296 your own circumstances, taking into account such factors as the
297 durability of the electronic record media and how long you are required by predicate rule
298 to maintain a particular electronic record. Below, we describe two approaches to
299 maintaining electronic records. We recognize that, within a given organization, you may
300 use one or both approaches, or another approach that meets applicable statutory and
301 regulatory requirements.

302 *6.1 The Time Capsule Approach*

303 The electronic records time capsule approach involves preserving an electronic record on

305 the same electronic media and computer system used to create the electronic record in the
306 first place. During the records retention period the computer system might be in use or it
307 might be inactive but still be capable of working. Throughout the records retention
308 period, you would keep the computer system functional and make no changes to the
309 computing environment. For example, you would not upgrade application and operating
310 software, or hardware; upgrades would constitute a migration, an approach explained
311 below. In short, you would maintain systems as they were at the time the electronic
312 records were created.

313 Under the time capsule approach, you should preserve system documentation, and ensure
314 that personnel are proficient in system operation and routine upkeep. This means that
315 personnel who are not familiar with a maintained older system should be trained
316 accordingly.

317 This approach may be of limited practicality for long-term maintenance of electronic
318 records due to the rapid pace of technology changes, such as the emergence of new
319 storage media, revisions to application and operating software, and hardware
320 modifications. In addition, companies that originally furnished systems used to create the
321 electronic records might not elect or be able to support the systems in the long term.
322 Nonetheless, the time capsule approach might be a viable option in some instances (e.g.,
323 where record retention periods are relatively short or the electronic record is created,
324 modified, maintained, or transmitted, on a relatively low cost computing system that is
325 dedicated to creating, modifying, maintaining, or transmitting the electronic record).

327 *6.2 The Electronic Records Migration Approach*

328 The electronic records migration approach involves moving electronic records
329 (migrating them) from one computing environment (the source or "old" system) to
330 another different computing environment (the destination or "new" system). You might
331 perform several successive migrations during the records retention period. The outcome
332 of the migration is an electronic record that continues to conform to
333 established regulatory and statutory requirements, including those identified above in
334 Section 4 of this document. You should document the migration so that
335 you have a traceable history of what systems were used throughout the records retention
336 period.

337 Upon completion and verification of a migration, you may elect to retire or discard the
338 old electronic records and/or system, provided that the migrated records meet all
339 requirements of the applicable predicate rules. However, you should
340 carefully consider when it would be prudent to discard the old electronic records and/or
341 system. The reason for this is that there is a risk that after the migration, a previously
342 unknown problem with the old electronic record or system might come to light. The
343 nature of the problem might adversely affect, among other things, the old electronic
344 record's accuracy, completeness, or authenticity. Your ability to solve the problem might
345 be hampered if you no longer have the old electronic record or system. (For example,
346 solving the problem might involve installing modifications specifically intended to be
347 made to the old system software, but not intended for the new system software.)
348 During a migration, one or more of the factors that enable an electronic record to

350 reliably preserve and present information might differ between old and new systems. For
351 example, a migration might typically involve transforming the digital sequence of
352 information (e.g., bits) that comprises the original (old) electronic record. It is important
353 to recognize differences between systems and how they might affect how reliably the
354 migrated electronic record can preserve and present information.

355 Changes in factors that affect how reliably an electronic record can preserve and present
356 information might not always be readily apparent. Examples of such changes include, but
357 are not limited to, the following:

358 • Installing a new version of an application or operating system software
359 program;
360 • Moving from one type of record storage media to a different one;
361 • Moving from one electronic file format to another;
362 • Changing from one type of video display unit or printer to another; and,
363 • Changing audio devices

364 6.2.1 Key Principles Of Electronic Records Migration

365 A migration generally involves a transformation of the original (old) electronic record.
366 You should be aware that without careful control, information might be lost or altered in
367 ways that impact such key factors as the electronic record's accuracy, completeness,
368 authenticity, integrity, and (potentially) confidentiality. In addition, without careful
369 control, the ability to process information might be adversely affected. We therefore

371 believe that it is extremely important that you plan and conduct the migration carefully,
372 and maintain the electronic record's ability to reliably preserve and present information.
373 Accordingly, you should carefully implement the principles set forth below in this
374 section.

375 6.2.1.1 Information Continuity Should Be Preserved.

376 We believe it is extremely important that the migrated electronic record in its new
377 computing environment conveys an accurate and complete representation of events, data,
378 actions, and identification and signatures of people as required by
379 the relevant predicate rule. Someone who reviews the migrated electronic record should
380 be able to reconstruct events to determine if the predicate rule was followed (e.g., who
381 did what, when, how, production values and conditions, study observations and findings).
382 If you do not maintain this continuity of information you might be violating the predicate
383 rule and you might not have sufficient information to detect, correct, and prevent
384 problems (e.g., problems relating to production and control of a regulated product).

385 6.2.1.2 Factors In The New Computer System That Enable The Electronic Record To
386 Reliably Preserve and Present Information Should Be Identified And
387 Controlled.

388 These factors include, but are not limited to:

389 • Data; we consider it extremely important that information in the migrated

391 electronic record be accurate and complete. For example, where an old
392 system electronic record included the body weights for 100 laboratory
393 animals, the migrated electronic record should contain the same information for
394 the same number of animals.

395 • Metadata; the information in the migrated electronic record that gives
396 context, meaning, and security attributes to the data should not lessen the
397 liability of the information the electronic record preserves and presents, even
398 though the metadata may have been transformed so that it functions properly in
399 the new system. For example, if a database is migrated to a new system, the new
400 data dictionary might differ from the old, but it should, nonetheless, accurately
401 and completely present the migrated information.

402 • Hardware; electronic record storage and display devices can affect the
403 reliability of information preserved and presented. For example, it is
404 possible for a new system video display that differs from the old system
405 video display in resolution or color fidelity to alter the reviewer's
406 interpretation of information (e.g., where graphics and text are color coded to
407 convey meaning and differentiate information).

408 • Software; the operating system and application programs of the new
409 system should maintain at least the same level of reliability in preserving
410 and presenting information as did the operating system and application
411 programs in the old system.

413 6.2.1.3 Electronic Record Integrity Attributes Should Be Preserved.

414 In designing and implementing an electronic record migration you should keep in mind
415 requirements (from part 11 as well as applicable predicate rules) for preserving
416 information that establishes record integrity. Electronic record integrity information
417 might be separate from, but associated with, an electronic record, and therefore
418 inadvertently overlooked if you only focused on migrating the electronic record itself.
419 This electronic record integrity information includes, but might not be limited to, audit
420 trails and links between signatures and electronic records. For example, section 11.10(e)
421 of part 11 requires that audit trails record all operator entries and actions that create,
422 modify or delete electronic records. Where a migration, in effect, creates a new electronic
423 record (by transforming the old electronic record) then, per section 11.10(e), the audit
424 trail for the migrated electronic record would have to cover this creation. By adding this
425 new creation step to the migrated audit trail carried over from the old electronic record
426 you will help ensure a continuity of electronic record integrity.

427 An audit trail itself may undergo a transformation during a migration, but keep in mind
428 that section 11.10(e) requires that the audit trail convey certain information, including
429 information about the creation, modification, and/or deletion of the old electronic record.

430 With respect to the part 11 requirement that signatures be linked to their respective
431 electronic records, the signature to electronic record links in the new electronic record
432 system might be created by a technology that differs from that used to create the links in
433 the old system. However, to meet part 11 requirements, it is important that the new links

435 "ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify
436 an electronic record by ordinary means." (See section 11.70.) By having reliable
437 signature to electronic record links in the new computer system, you will help establish
438 continuity of electronic record integrity.

439 6.2.1.4 The Ability To Process Information In Electronic Records Should Be
440 Preserved.

441 The importance of being able to process information in an electronic record, using
442 computer technologies, is explained above. In the migration approach, the
443 new computer system should enable you to search, sort and process information in the
444 migrated electronic record at least at the same level as what you could attain in the old
445 system (even though the new system may employ different hardware and software). For
446 example, if you could sort a table of values using the old system, you should be able to
447 sort those values in the migrated electronic record using the new system, and achieve the
448 same results. Some new systems can, by emulating older systems, process information in
449 a very similar way.

450 6.2.1.5 Unavoidable Differences And Losses Should Be Accounted For and
451 Explained In The Migrated Electronic Record Or New System Documentation.

452 When electronic records are migrated from one system to another, we recognize that
453 there might be unavoidable losses or changes in certain information or record attributes
454 that do not diminish the reliability of information that is preserved and presented. It

456 should be clear that this caveat does not apply to losses or changes in information
457 specifically mandated by predicate rules. In addition, we note that changing a record's
458 content could undermine its authenticity. Generally, our view is that the migrated
459 electronic record could still reliably preserve and present information, despite some
460 losses or modifications, provided that differences are appropriately accounted for, and
461 explained in either the migrated record or readily available electronic documentation.
462 Here are some examples:

463 • Digital signature verification: current technical methods of verifying a digital
464 signature depend upon maintaining the "as signed" electronic record in an
465 unaltered state. The automated digital signature verification process will yield a
466 "failure" outcome (indicating that the contents of the electronic record changed
467 after the record was signed, or that the signature is not genuine) if the migrated
468 electronic record is in a different file format or otherwise not identical in every
469 respect. To account for this scenario, yet ensure continuity of record integrity,
470 you should perform the following sequence of procedures:

471 ♦ Just prior to performing the electronic record migration a trusted
472 third party from outside of the organization that has some
473 responsibility for the electronic record verifies the digital
474 signature using the old system methods;

475 ♦ Under supervision of the above trusted third party, the signed
476 electronic record is migrated to the new system; and,

- The above trusted third party then applies a new digital signature (using technologies appropriate to the new system) to the migrated electronic record. The same third party also prepares and applies a digital signature to a new separate electronic record (or to an addition to the migrated electronic record) that explains the migration. In this situation, although you would no longer be able to verify the old digital signature directly, you should nonetheless be able to demonstrate continuity of record integrity by verifying the newly digitally signed migrated electronic record and explanatory statement.

- Color code changes; the electronic record in an old system includes a chart that uses colors to describe different groups of test animals, and the text accompanying the chart refers to the groups by those colors. The new system cannot replicate those colors; it uses a different set of colors to represent information. In this case, the migrated electronic record should use the new color representations to differentiate the groups so that the information and distinctions made in the old electronic record are maintained fully and accurately. An electronic record that supplements the migrated electronic record should explain the correlation between old and new color representations, so that the reader would correctly interpret the information. However, text (that referred to the colors) in the migrated electronic record should not be altered because doing so would change the record content and authenticity.

7. APPENDIX – References

You may find the following publications of interest with respect to electronic records maintenance.

Dr. Luciana Duranti, Principal Investigator, University of British Columbia, *"The Preservation of The Integrity of Electronic Records,"* March, 1997 (Internet address:http://www.slais.ubc.ca).

Alabama Department of Archives and History, *"Guidelines For The Use Of Digital Imaging Technologies For Long-Term Government Records In Alabama,"* April, 1997 (Internet address: http://www.archives.state.al.us/ol_pubs/digital.html).

National Institute of Standards and Technology, U.S. Department of Commerce, *"An Introduction to Computer Security: The NIST Handbook,"* Special Publication 800-12.

National Archives and Records Administration, *"Records Management Guidance for Agencies Implementing Electronic Signature Technologies"*, October 18, 2000.

Gregory S. Hunter, *"Preserving Digital Information, A How-To-Do-It Manual"*, How-To-Do-It Manuals For Librarians, Number 93, Neal-Schuman Publishers, Inc. 2000.

DLM Forum, European Communities, *"Guidelines On Best Practices For Using Electronic Information,"* 1997 (Internet address: http://www.echo.lu/dim/en/home.html).

519 *"Electronic Signatures in Global and National Commerce Act,"* Public Law 106-229, 14
520 Stat 464 .(Internet address: http://thomas.loc.gov/cgi-bin/bdquery/z?d106:SN00761).

521 U.S. Department of Defense, *"Design Criteria Standard For Electronic Records*
522 *Management Software Applications,"* DOD 5015.2-STD, November 1997.

523 Doc ID: MaintenanceGuidanceDraft_postRES.doc
524 08/29/02